Quantum Inf Process (2014) 13:1–4
DOI 10.1007/s11128-013-0719-1

EDITORIAL

Introduction to Special Issue on quantum cryptography

Gerald Gilbert · Yaakov S. Weinstein

Published online: 3 January 2014

The problem of private communication in the presence of an eavesdropper has been studied for centuries. While various techniques have been explored, a complete solution has been proven possible only 30 years ago. This solution has two basic components: the one-time pad and quantum key distribution (QKD). The one-time pad is an encoding method that can achieve unconditionally secret communications if the sender and receiver share a secret key, a random sequence of symbols with which a message can be encoded. A secret key can be generated (even in the presence of an eavesdropper) using QKD. Together, the one-time pad and QKD provide a completely secret end-to-end cryptosystem: key distribution *via* QKD followed by encryption of the desired message using the key material as a one-time pad.

An example of a complete cryptographic system is shown in Fig. 1 and can be described as follows. Alice wishes to send a message M to Bob. She encodes the message using a shared key K via transformation T_K. The encoded message E is sent to Bob but during the transmission an eavesdropper Eve, assumed to have unlimited resources being bound only by the laws of physics, will attempt to decipher the message. Bob receives the message and, utilizing the key he and Alice share, decodes the message.

Thus we see that Alice must share two blocks of information with Bob, the encoded message and the key. For cryptography to work properly Eve must be unable to decode the message despite complete knowledge of E. This means that Eve, despite her unlimited computational power, must be unable to determine the key, K.

There are numerous possible key types that can and have been used. However, only the one-time pad achieves unconditional secrecy by encoding the message with a truly random key [1]. Let us assume an alphabet consisting of two letters, 0 and 1. To encode

G. Gilbert (✉) · Y. S. Weinstein
Quantum Information Science Group, MITRE, 200 Forrestal Rd., Princeton, NJ 08540, USA
e-mail: ggilbert@mitre.org

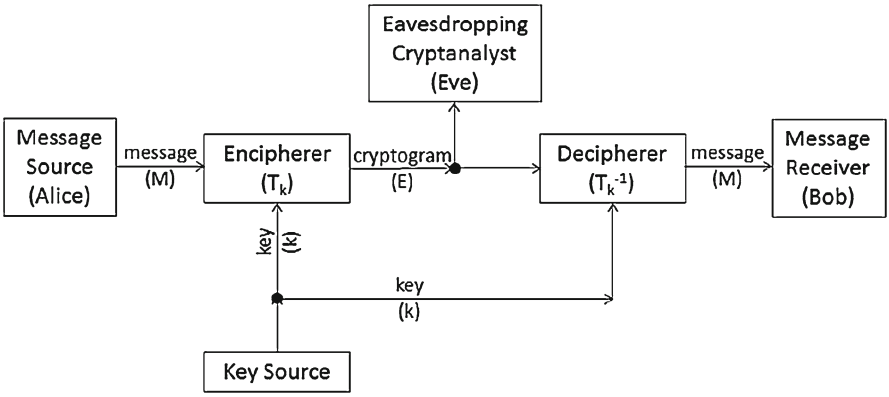

Fig. 1 Schematic of a cryptographic system (based on Shannon)

a message, the one-time pad applies the "exclusive or" (XOR) logic operation, between the key and the message resulting in another random string. Thus, the encoded message cannot be decrypted without the key. The one-time pad is extremely expensive, it costs one bit of information to encode one bit of the message. Nevertheless, it is the only known way to achieve unconditionally secret communications.

The first protocol to achieve QKD was developed by Bennett and Brassard [2] and is known as the "BB84" protocol. To achieve secure key distribution Alice and Bob publicly agree to make use of photons in two different polarization bases. The bases are chosen to be maximally non-orthogonal and each individual photon is prepared in one of the four randomly chosen polarization states. Alice transmits the photons which are measured by Bob in one or the other of the polarization bases. The choices of basis is again random. About half the time the basis choices of Alice and Bob will be the same. The two parties publicly compare their choice of basis for each transmitted photon but do not reveal the states that were transmitted or observed. The bits from the cases where the bases agree furnish the "sifted key." The Heisenberg Uncertainty Principle now guarantees that an eavesdropper cannot measure the polarizations during transmission without being detected. Error correction is then applied to the sifted keys to fix errors caused by imperfect equipment. In addition, a hash function-based protocol known as "privacy amplification" is utilized to reduce the information gained by Eve due to the presence of multiple photon states.

Since the introduction of BB84 many other QKD protocols have been discovered and continue to be discovered. This Special Issue includes a new protocol by Kang et al. Their protocol is an asymmetric version of the "4+2" protocol [3] that may be viable over longer distances in a lossy channel.

Today, in addition to QKD, there are many other known secure communications protocols which exploit quantum phenomena. One of the first of these protocols was quantum secret sharing (QSS) [4] which itself can be implemented in numerous ways. In secret sharing, a message is divided into several parts and each part is sent to a different agent. All, or a specified subset, of the parts are needed to reconstruct the original secret. In QSS both the secret information splitting and the transmission of the parts

are done by exploiting quantum mechanical phenomena. In this Special Issue there are three papers with relevance to QSS. The first, by Chen et al., generalizes the two-party Cascade error-correction protocol for QKD [5] into a protocol for multiple parties. This allows for the practical implementation of multi-party QSS. The second, by Shi, et al., details a one-insider (one of those receiving a part of the secret) attack that will break a specific QSS protocol. The third by Xu et al., addresses aspects of hierarchical quantum information splitting, a protocol in which the quantum information is broken up in such a way that some subset of agents have greater access to the secret than other agents [6]. The developed protocol is for an arbitrary two-qubit state, and allows for multiple agents such that the "high grade" agents need only each other and one "low grade" agent to reconstruct the secret while the low grade agents need cooperation from everyone. In addition, the agents need only singe-qubit measurements.

As explained above, QKD allows two parties to construct a cryptographic key which can later be used for secure cryptography. Subsequent to the discovery of QKD, protocols were developed in which actual messages can directly be secretly transmitted. One class of these protocols is deterministic secure quantum communication (DSQC) [7]. In this Special Issue, Srinatha et al., introduce an exciting advancement in DSQC which they call the quantum cryptographic switch. The switch allows Alice to send information to Bob who can only recover the information with permission of a third party. The third party can continuously vary the amount of informaiton Bob can recover.

Another important branch of secret quantum communications is quantum versions of secure multiparty computation and, specifically, private comparison. In private comparison information of two parties is compared and determined to be equal or not without revealing the actual information. As with QSS, numerous quantum private comparison (QPC) protocols have been developed [8]. A new protocol for QPC is detailed in Special Issue. Liu et al., propose a QPC method based on differential phase shift QSS. This protocol is more experimntally feasible than previous protocols since it utilizes weak coherent pulses in place of entangled or single photons. Another interesting class of QPC protocols is developed by Chen et al. These protocols utilize symmetric states and require the players to implement only Pauli operations and the third party to only prepare the initial state and perform measurements. Finally this Special Issue includes a QPC protocol developed by Chen et al., which utilizes single photons and can be successfully performed in an amplitude damping channel.

Quantum signatures guarantee the authentication of and the undeniability of a signature to a classical message [9]. A variant of this is the arbitrated quantum signature (AQS) in which a receiver obtains a quantum signature *via* a trusted arbitrator. In this Special Issue, Luo and Hwang note a flaw in previous AQS protocols: the assumption of an authenticated classical channel. They then propose a new AQS scheme which does not use such a channel and is nonetheless secure against the Trojan-horse and other attacks. Another variant of quantum signatures is that of the quantum blind signature. In a blind signature the signer is not aware of the message content and the message owner cannot remove the signature. A third party can verify the signature thus ensuring that the message has not been changed. In this Special Issue Khodambashi and Zakerolhosseini construct a complete quantum blind signature protocol and demonstrate that it is unconditionally secure.

Not every protocol can be strengthened *via* quantum cryptographic methods. However, quantum cryptographic techniques may be able to increase security in certain scenarios. For example, it is known that quantum oblivious transfer (QOT) is theoretically not secure (without additional assumptions). Nevertheless, quantum protocols have been developed that can lead to practical effective QOT based on today's technology. In this Special Issue Li et al., improve on these protocols by designing a QOT protocol that is loss-tolerant and allows for error correction. Similarly, unconditionally secure quantum bit commitment (QBC) has been shown impossible for non-relativistic scenarios. Nonetheless, QBC can work for certain security models. In this Special Issue Li et al., formulate a cheat sensitive QBC protocol in which any cheating strategy will be detected with non-zero probability. The novelty of their protocol lies in the utilization of pre- and post-selected quantum states.

Finally, this Special Issue features a paper by Thilagam exploring the relationship between measurement attributes, such as precision and the amount of time the measurement takes, and correlations between a pair of qubits. While not explicitly addressing quantum cryptographic protocols, this work may have relevance to the security of certain protocols as the eavesdropper must perform a measurement in order to gain information.

The field of quantum cryptography continues to blossom. New applications continue to be discovered and new protocols continue to improve older applications. Studies of other areas of quantum information science help stimulate some of these new approaches. This Special Issue attempts to highlight some of these trends.

It is a pleasure to thank Dr. Howard Brandt and the staff of Quantum Information Processing for inviting us to serve as Guest Editors for this issue and guiding us at every turn. In addition, we would like to thank those who contributed to this Special Issue for their high-quality work. We hope that readers of this issue will gain renewed appreciation and insight into the multi-faceted area of quantum cryptography.

References

1. Shannon, C., Weaver, W.: The Mathematical Theory of Communication. University of Illinois Press, Champaign, IL (1971)
2. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, 175 (1984)
3. Huttner, B., Imoto, N., Gisin, N., Mor, T.: Quantum cryptography with coherent states. Phys. Rev. A **51**, 1863–1869 (1995)
4. Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829–1834 (1999)
5. Brassard, G., Salvail, L.: Secret-key reconciliation by public discussion. In: Lecture Notes in Comput. Sci. vol. 765, pp. 410–423 (1994)
6. Wang, X.W., Xia, L.X., Wang, Z.Y., Zhang, D.Y.: Hierarchical quantum-information splitting. Opt. Commun. **283**, 1196–1199 (2010)
7. Shimuzu, K., Imoto, N.: Communcation channels secured from eavesdropping via transmission of photonic Bell states. Phys. Rev. A **60**, 157–166 (1999)
8. Yang, Y.G., Wen, Q.Y.: An efficient two-party quantum private comparison protocol with decoy states and two-photon entanglement. J. Phys. A **42**, 055305 (2009)
9. Gottesman, D., Chuang, I.: Quantum digital signatures arXiv:quant-ph/0105032v2 (2001)